НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
КАФЕДРА МАТЕМАТИЧНИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ

«На правах рукопису»
УДК _____

«До захисту допущено»
В.о. завідувача кафедрою
_____ М.М.Савчук
(підпис) (ініціали, прізвище)
“___” _____ 2018р.

Магістерська дисертація

на здобуття ступеня магістра

зі спеціальності 113 «Прикладна математика» _____
(код і назва)

на тему: Аналіз та обґрунтування взаємозв’язку між кривими у формі Монтгомері та у формі Едвардса. _____
_____
_____

Виконав (-ла): студент (-ка) __2__ курсу, групи ФІ-73 мп
(шифр групи)

Вихло Антон Андрійович _____ _____
(прізвище, ім’я, по батькові) (підпис)

Керівник професор, к.т.н. Ковальчук Л.В._____ _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант _____ _____ _____
(назва розділу) (науковий ступінь, вчене звання, , прізвище, ініціали) (підпис)

Рецензент_____ _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2018року

Національний технічний університет України
«Київський політехнічний інститут
імені Ігоря Сікорського»
Фізико-технічний інститут
Кафедра математичних методів захисту інформації

Рівень вищої освіти: другий (магістерський) за освітньо–професійною програмою

Спеціальність: 113 «Прикладна математика»

ЗАТВЕРДЖУЮ
В.о. завідувача кафедрою
_____ М.М.Савчук
(підпис) (ініціали, прізвище)
«___»_____201_ р.

ЗАВДАННЯ
на магістерську дисертацію студенту

Вихло Антону Андрійовичу
(прізвище, ім'я, по батькові)

1. Тема дисертації Аналіз та обґрунтування взаємозв'язку між кривими у формі Монтгомері та у формі Едвардса _____
_____
_____ ,
науковий керівник дисертації Ковальчук Людмила Василівна, професор, к.т.н,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від _____р. № _____

2. Термін подання студентом дисертації _____

3. Об'єкт дослідження – процес перетворення еліптичної кривої у довільній формі в еліптичну криву в формі Едвардса. _____
_____

4. Предмет дослідження (Вхідні дані – для магістерської дисертації за освітньо–професійною програмою)
Перетворення еліптичної кривої в формі Монтгомері в еліптичну криву в формі Едвардса _____
_____
_____

5. Перелік завдань, які потрібно розробити _____
_____
_____

_____

_____

_____

6. Орієнтовний перелік ілюстративного матеріалу _____

_____

_____

7. Орієнтовний перелік публікацій _____

_____

_____

8. Консультанти розділів дисертації*

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

9. Дата видачі завдання _____

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка

Студент _____ _____

(підпис) (ініціали, прізвище)

Науковий керівник дисертації _____ _____

(підпис) (ініціали, прізвище)

* Консультантом не може бути зазначено наукового керівника магістерської дисертації.

РЕФЕРАТ

Кваліфікаційна робота містить: 59 стор., 10 джерел.

Метою кваліфікаційної роботи є визначити необхідні і достатні умови існування кривої у формі Едвардса, що є ізоморфною до заданої кривої у формі Монтгомері.

Для досягнення мети необхідно розв'язати такі **задачі дослідження**, які полягають формулюванні необхідних і достатніх умов існування кривої у формі Едвардса, що є ізоморфною до заданої кривої у формі Монтгомері, обчисленні кількості таких кривих у формі Монтгомері та програмній реалізації розробленого алгоритму перетворення.

Об'єктом дослідження є процес перетворення еліптичної кривої у довільній формі в еліптичну криву в формі Едвардса.

Предметом дослідження є перетворення еліптичної кривої у формі Монтгомері в еліптичну криву в формі Едвардса.

У ході роботи було виконано:

1) отримано, строго доведені, необхідні і достатні умови існування кривої у формі Едвардса, що є ізоморфною до заданої кривої у формі Монтгомері;

2) обчислено кількість кривих у формі Монтгомері, що є ізоморфними кривими Едвардса;

3) розроблено алгоритм, що виконує ізоморфне перетворення (при виконанні умов ізоморфізму) кривої у формі Монтгомері у криву у формі Едвардса;

4) Реалізовано розроблений алгоритм.

ЕЛІПТИЧНІ КРИВІ ЕДВАРДСА, ЕЛІПТИЧНІ КРИВІ МОНТГОМЕРІ, ПЕРЕТВОРЕННЯ ЕЛІПТИЧНИХ КРИВИХ, ІЗОМОРФІЗМ

РЕФЕРАТ

Квалификационная работа содержит 59 стр., 10 источников.

Целью квалификационной работы является определение необходимые и достаточные условия существования кривой в форме Эдвардса, что является изоморфной к заданой кривой в форме Монтгомери, исчислению количества таких кривых в форме Монтгомери и програмной реализации разработаного алгоритма преобразование.

Объектом исследования является процесс преобразование эллиптической кривой в произвольной форме в эллиптическую кривую в форме Эдвардса.

Предметом исследования является превращение эллиптической кривой в форме Монтгомери в эллиптическую кривую в форме Эдвардса.

В ходе работы было выполнено:

1) получено, стого доказаные, необходимые и достаточные условия существования кривой в форме Эдвардса, что является изоморфной к заданой кривой в форме Монтгомери.

2) получено количество кривых в форме Монтгомери, что являются изоморфными к кривым Эдвардса.

3) разработан алгоритм, что выполняет изоморфное преобразование (если выполняются условия изоморфизма) кривой в форме Монтгомери в кривую в форме Эдвардса;

4) программную реализацию полученного алгоритма;

ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ ЭДВАРДСА, ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ МОНТГОМЕРИ, ПРЕОБРАЗОВАНИЕ ЭЛЛИПТИЧЕСКИХ КРИВЫХ, ИЗОМОРФИЗМ

ABSTRACT

The qualification work contains 59 pages, 10 sources.

The purpose of qualifying work is to determine the necessary and sufficient conditions for the existence of a curve in the form of Edwards, which is isomorphic to a given curve in the form of Montgomery, the calculation of the number of such curves in the form of Montgomery and the software implementation of the developed conversion algorithm.

Object of study is the process of transforming an elliptic curve in any form into an elliptic curve in the form of Edwards.

Subject of research is the transformation of an elliptic curve in the form of Montgomery into an elliptic curve in the form of Edwards.

In the course of the work was performed:

1) obtained, just proved, necessary and sufficient conditions for the existence of a curve in the form of Edwards, which is isomorphic to a given curve in the form of Montgomery.

2) obtained the number of curves in the form of Montgomery, that are isomorphic to Edwards curves.

3) an algorithm is developed that performs an isomorphic transformation (if the isomorphism conditions are fulfilled) of a curve in the form of Montgomery into a curve in the form of Edwards;

4) software implementation of the resulting algorithm;

EDWARDS ELLIPTIC CURVES, MONTGOMERY ELLIPTIC CURVES, ELLIPTIC CURVE TRANSFORMATION, ISOMORPHISM

ЗМІСТ

ВСТУП

Актуальність дослідження. Актуальність даного дослідження полягає у тому, що еліптичні криві в формі Едвардса над простим полем на теперішній час є найбільш швидкими та перспективними для використання в асиметричних криптосистемах. Особливо важливі такі властивості як рекордна швидкість, універсальність закону додавання, а також можливість представлення нейтрального елемента в афінних координатах.

Метою дослідження є визначити необхідні і достатні умови існування кривої у формі Едвардса, що є ізоморфною до заданої кривої у формі Монтгомері.

Для досягнення мети необхідно вирішити такі завдання:

1) отримати, строго доведені, необхідні і достатні умови існування еліптичної кривої у формі Едвардса, що є ізоморфною до заданої кривої у формі Монтгомері;

2) обчислити кількість кривих у формі Монтгомері, що є ізоморфними кривими Едвардса;

3) розробити алгоритм, що виконує ізоморфне перетворення (при виконанні умов ізоморфізму) кривої у формі Монтгомері у криву у формі Едвардса;

4) Реалізовати розроблений алгоритм.

Об'єктом дослідження є процес перетворення еліптичної кривої у довільній формі в еліптичну криву в формі Едвардса.

Предметом дослідження є перетворення еліптичної кривої у формі Монтгомері в еліптичну криву в формі Едвардса.

При розв'язанні поставлених завдань використовувались такі *методи дослідження*: абстрактна та прикладна алгебра, теорія складності обчислень, програмування.

Наукова новизна отриманих результатів полягає формулюванні

необхідних та достатніх умов існування еліптичної кривої у формі Едвардса, що є ізоморфною до заданої кривої у формі Монтгомері.

Практичне значення результатів полягає формалізації алгоритму ізоморфного перетворення еліптичної кривої в формі Монтгомері в еліптичну криву в формі Едвардса

1 ЕЛІПТИЧНІ КРИВІ

В цьому розділі приведено огляд еліптичних кривих. Розглянуто такі форми еліптичних кривих як форма Вейєрштрасса, узагальнена форма Вейєрштрасса і форма Монтгомері, та базові факти про них.

1.1 Базові поняття

Еліптичні криві є об'єктом інтенсивних досліджень останні 90 років. Основною причиною цьому є те, що еліптичні криві над скінченним полем мають високу швидкість обчислень за рахунок їх структури. Еліптичні криві є аналогом мультиплікативних груп над полями, але вони мають перевагу гнучнкості вибору в порівнянні з вибором скінченного поля.

Нехай F - будь-яке поле. Тоді *еліптичною кривою над полем* F називається крива, що задається рівнянням виду

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1.1}$$

Позначимо через $E(F)$ множину, що складається з точок $(x, y) \in F^2$, що задовольняють цьому рівнянюю і точки на нескінченності O. Якщо K - деяке розширення поля F, тоді через $E(K)$ буде позначатись множина, що складається з точок $(x, y) \in K^2$, шо задовольняють рівнянню 1.1 і точки на нескінченності O.

Якщо характеристика поля $F \neq 2$, то лінійною заміною змінних $y \to y - \frac{a_1x+a_3}{2}$ крива 1.1 приводиться до вигляду

$$y^2 = x^3 + a_2x^2 + a_4x + a_6 \tag{1.2}$$

Якщо K - поле характеристики $\neq 2{,}3$, то без втрати загальності можна покласти коефіцієнт $a_2 = 0$, з рівняння 1.2.

Таким чином рівняння еліптичної кривої приймає вигляд

$$y^2 = x^3 + ax + b, a, b \in F \tag{1.3}$$

Умовою гладкості в цьому випадку є те, що кубічний многочлен

$$f(x) = x^3 + ax + b, \tag{1.4}$$

не має кратних коренів.

Якщо F - поле характеристики 2, тоді *еліптичною кривою над* F називається набір точок, що задовольняють рівнянню

$$y^2 + cy = x^3 + ax + b, \tag{1.5}$$

або

$$y^2 + xy = x^3 + ax^2 + b, \tag{1.6}$$

разом з точкою на нескінченності.

Якщо F - поле характеристики 3, тоді *еліптичною кривою над* F називається набір точок, що задовольняють рівнянню

$$y^2 = x^3 + ax^2 + bx + c, \tag{1.7}$$

разом з точкою на нескінченності.

Перед тим, як розглядати специфічні приклади еліптичних кривих над різними полями, необхідно зазначити центрально важливу властивість про набір точок еліптичної кривої над полем дійсних чисел: вони формують абелеву групу.

1.2 Еліптичні криві в формі Вейєрштрасса

Найбільш відомою формою еліптичної кривої є форма Вейєрштрасса, що задається наступним рівнянням:

$$y^2 = x^3 + Ax + B, \tag{1.8}$$

де A та B - константи.

Необхідно зазначити до яких множин відносяться параметри A, B, x та y. Зазвичай, вони можуть братись як елементи полів, наприклад, дійсних чисел R, комплексних чисел C, раціональних чисел Q, одним з скінченних полів F_q, де $q = p^k$, де $k \geq 1$.

Якщо K - поле, $A, B \in K$, тоді ми кажемо, що E задана над полем K.

Якщо ми хочемо задати точки координатами якогось поля $L \supseteq K$, то можемо позначити це як $E(L)$. За означенням цей набір завжди містить в собі точку на нескінченності O:

$$E(L) = \{O\} \cup \{(x, y) \in L \times L \mid y^2 = x^3 + Ax + b\}. \tag{1.9}$$

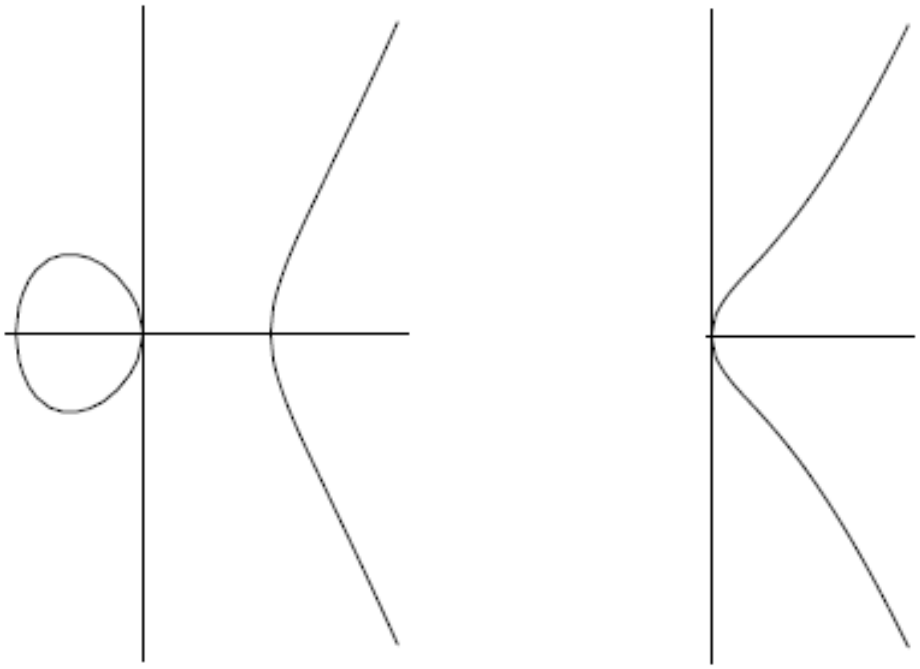
Для еліптичних кривих над більшістю полів неможливо зобразити інформативний графік. Але має сенс пам'ятати який вигляд має графік еліптичної кривої заданої над дійсними числами. Ці два базові графіки зображено на 1.1. Кубічне рівняння $y^2 = x_x^3$ має лише один дійсний корінь.

Що трапляється коли це рівняння має декілька коренів? Це не допускається. Фактично, припускається, що:

$$4A^3 + 27B^2 \neq 0. \tag{1.10}$$

Якщо корені кубіки це $((r_1 - r_2)(r_1 - r_3)(r_2 - r_3))^2 = -(4A^3 + 27B^2)$.

Випливає, що корені кубічного рівняння мають бути різними.



(а) $y^2 = x^3 - x$ **(б)** $y^2 = x^3 + x$

Рисунок 1.1

1.3 Еліптичні криві в узагальненій формі Вейєрштрасса

З метою мати більшу гнучкість, означено більш загальне рівняння еліптичної кривої в формі Вейєрштрасса.

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1.11}$$

де $a_1, ..., a_6$ - константи. Ця більш загальна форма є корисною для роботи з полями характеристистики 2 і характеристики 3. Якщо характеристика поля не дорівнює 2, тоді ми можемо поділити на 2 і виконати піднесення до квадрату:

$$\big(y + \frac{a_1x}{2} + \frac{a_3}{2}\big)^2 = x^3\big(a_2 + \frac{a_1^2}{4}x^2\big) + \big(a_4 + \frac{a_1a_3}{2}\big)x + \big(\frac{a_3^2}{4} + a_6\big) \tag{1.12}$$

це може бути записано як:

$$y_1^2 = x^3 + a_2'x^2 + a_4'x + a_6', \tag{1.13}$$

де $y_1 = y + a_1x/2 + a_3/2$ та a_2', a_4', a_6' - константи. Якщо характеристика також не дорівнює 3, тоді ми можемо покласти $x_1 = a_2'/3$, звідки ми можемо отримати

$$y_1^2 = x_1^3 + Ax_1 + B, \tag{1.14}$$

де A, B - константи.

1.4 Еліптичні криві в формі Монтгомері

Нехай q - просте число та F_q - скінченне поле. Еліптична крива в формі Монтгомері над F_q задається наступним рівнянням:

$$E_{a,b} : by^2 = x(x^2 + ax + 1), \tag{1.15}$$

де a, b - параметри кривої, що задовольняють наступним вимогам: $a, b \in F_q, b \neq 0, a^2 \neq 4$, що відповідають за вимоги несингулярності.

Еліптична крива в формі Монтгомері визначається параметрами a, b. Слід зазначити, що параметр a контролює геометрію кривої, а параметр b є фактором кручення.

Розглянемо операції на еліптичній кривій в формі монтгомері для афінних координат. Нехай $P = (x_1, y_1), Q = (x_2, y_2)$- точки кривої. Тоді закон додавання задається наступною формулою:

$$(x_1, y_1) + (x_2, y_2) = (b\lambda^2 - a - x_1 - x_2, \lambda(x_1 - x_3) - y_1), \tag{1.16}$$

де $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$

А закон подвоєння, відповідно, визначається наступною формулою:

$$2(x_1, y_1) = (b\lambda^2 - a - 2x_1, \lambda(x_1 - x_3) - y_1), \tag{1.17}$$

де $\lambda = \frac{3x_1^2+2ax_1+1}{2by_1}$

Висновки до розділу 1

В цьому розділі були описані та класифіковані еліптичні криві, зокрема еліптичні криві у формі Монтгомері та у класичній і узагальненій формах Вейєрштрасса. Були розглянуті відмінності між різними формами еліптичних кривих.

2 ЕЛІПТИЧНІ КРИВІ В ФОРМІ ЕДВАРДСА

В цьому розділі описуються еліптичні криві в формі Едвардса, які вперше було описано в роботі [2], далі були вдосконалені в роботі [7], детальні шляхи розвитку криптосистем на таких кривих наведено в роботі [4]. Наведено їх математичний опис, властивості та характеристики, які роблять використання кривих в даній формі рекордно продуктивним.

2.1 Еліптичні криві в оригінальній формі Едвардса

В перших роботах Гарольда Едвардса[1] розглядались властивості еліптичної кривої в формі

$$x^2 + y^2 = e^2(1 + x^2y^2). \tag{2.1}$$

Едвардсу вперше вдалось довести, що рівняння (2.1) описує криву, ізоморфну кривій в формі Вейєрштрасса, і отримати закон додавання її точок

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + x_2y_1}{e(1 + x_1x_2y_1y_2)}, \frac{y_1y_2 - x_1x_2}{e(1 - x_1x_2y_1y_2)}\right). \tag{2.2}$$

Криві (2.1) називають оригінальною формою Едвардса. Зауважимо, що нейтральним елементом тут є точка $O = (0, 1)$

Криві (2.1) існують над всіма полями з ненулевою характеристикоою і над скінченними полями ${F_p}^m$ характеристики $p \neq 2$. При співпадінні точок, що додаються універсальним законом (2.2) отримуємо в частковому випадку закон подвоєння

$$2(x_1, y_1) = \left(\frac{2x_1y_1}{e(1 + {x_1}^2{y_1}^2)}, \frac{{y_1}^2 - {x_1}^2}{e(1 - {x_1}^2{y_1}^2)} \right) \tag{2.3}$$

Для задач криптографії є актуальними лише криві виду (2.1) над полем F_q скінченного порядку $q = p^m$. Очевидно, заміною $x \to \frac{x}{e}$ крива (2.1) записується в ізоморфній формі

$$x^2 + y^2 = 1 + e^4x^2y^2 \Rightarrow y^2 = \frac{1 - x^2}{1 - e^4x^2}, e^4 \neq 1. \tag{2.4}$$

При $e = 1$ при всіх значеннях x маємо два розв'язки $y = \pm 1$, і порядок такої кривої $N_E = 2q$ виходить за межі Хассе[7], крива не є еліптичною. Крім того, виникають особливі випадки в законі подвоєння точки. Наприклад, подвоєння точки $P = (1, 1)$, яка є розв'язком рівняння (2.1), породжує невизначеність $0/0$ для y - координати в (2.3). Тому потрібно прийняти $e^4 \neq 1$, тоді число значень рівняння (2.4) обмежується числом елементів e^4 поля, породжуючих квадрати в правій частині рівняння.

Для точки F_0 4-го порядку кривої приймаємо $2F_0 = D_0$, отримаємо відповідно 2.3

$$\frac{2x_1y_1}{e(1 + x_1^2y_1^2) = 0}, \frac{y_1^2 - x_1^2}{e(1 + x_1^2y_1^2) = -e}. \tag{2.5}$$

звідси $y_1^2 = 0 \to x_1^2 = e^2 \to x_1 = \pm e$ Отже, для кривої 2.1 при $e^4 \neq 1$ над скінченним полем характеристики $p \neq 2, 3$, завжди існують дві точки 4-го порядку $\pm F_0 = (\pm e, 0)$. Одразу помітимо, що знайденими вище не обмежуються всі точик 2-го і 4-го порядків. Наприклад, завжди є ще дві особливі точки 2-го порядку(на нескінченності), і крива 2.1 є нециклічною (з трьома точками 2-го порядку).

Дійсно, із рівняння кривої 2.1 справедливо

$$y^2 = \frac{e^2 - x^2}{1 - e^2x^2}, x^2 = \frac{e^2 - y^2}{1 - e^2y^2} \tag{2.6}$$

При нульових значеннях знаменників цих рівностей отримумо 4

особливі точки кривої: $F_{1,2} = (\pm e^{-1}, \infty), D_{1,2} = (\infty, \pm e^{-1})$. Тут під знаком "$\infty$" позначено ділення на 0. Хоча в скінченному полі ці елементи не означені, але в групових операціях 2.2, 2.3, що мають вигляд раціональних функцій, обидві координати точок входять в чисельники і знаменники. Це дозволяє використовувати формули 2.2 і 2.3 в особливих точках, приймаючи правила звичайного граничного переходу.

Тоді використовуючи 2.3 отримаємо

$$2D_{1,2} = 2(\infty, \pm e^{-1}) = \left(0, \frac{\infty^2}{ee^{-2}\infty^2}\right) = (0, e) = O. \tag{2.7}$$

$$2F_{1,2} = 2(\pm e^{-1}, \infty) = \left(0, \frac{\infty^2}{-ee^{-2}\infty^2}\right) = (0, -e) = O. \tag{2.8}$$

Звідси випливає, що особливі точки $D_{1,2}$ мають порядок 2, а сособливі точки $F_{1,2}$ мають порядок 4. Оригінальні криві Едвардса, таким чином, мають властивості нециклічних кривих.

Аналогічно, для точки S 8-го порядку з врахуванням рівняння $2S = F$ маємо

$$\frac{2x_1y_1}{e(1 + x_1^2y_1^2)} = e, \frac{y_1^2 - x_1^2}{e(1 - x_1^2y_1^2)} = 0. \tag{2.9}$$

Тоді з врахуванням 2.1

$$y_1^2 = x_1^2 \Rightarrow x_1^4 - 2e^{-2}x_1^2 + 1 = 0 \Rightarrow x_1^2 = e^{-2}(1 \pm \sqrt{1 - e^4}) \tag{2.10}$$

Тут ми бачимо, що точик 8-го порядку існують лише в тому випадку, коли вираз в дужках існує і є квадратом.

Основні відмінності кривої Едвардса у порівнянні з кривою Вейєрштраса:

1) Універсальність закону додавання.

2) Відсутність "точки на нескінченості". Так, нейтральним елементом є звичайна точка кривої Едвардса з координатами (0,1).

3) Група E_p завжди циклічна.

4) Порядок групи E_p завжди ділиться на 4. Цю властивість кривої Едвардса можна вважати її незначним недоліком у зв'язку з тим, що її підгрупа великого простого порядку, на базі якої будуються криптосистеми, буде мати як мінімум у 4 рази менше точок, ніж вся група, тобто як мінімум три чверті точок групи виявляються "зайвими".

5) Рекордна швидкість додавання точок. Ця властивість є однією з найсуттєвіших переваг кривої Едвардса.

6) Уніфікованість закону додавання точок. Формули додавання точок кривої Едвардса однакові і при подвоєнні точки, і при додаванні різних точок. Це підвищує стійкість криптосистем на кривих Едвардса до таймінгових та ємнісних атак, метою яких є визначення числа, на яке множиться точка кривої.

2.2 Еліптичні криві в формі Едвардса з модифікацією Бернштейна-Ланге

В роботі Даніеля Бернштейна[1], в якій запропонована модифікація кривої (2.1) з введенням 3 неквадратичного параметра d над скінченним полем F_pm характеристики $p \neq 2$ вигляду

$$x^2 + y^2 = e^2(1 + dx^2y^2), d(1 - de^4) \neq 0, (\frac{d}{p}) = -1, \tag{2.11}$$

де $(\frac{d}{p})$ – символ Лежандра, і параметр d – квадратичний лишок.

Універсальний закон додавання для точок цієх кривої має вигляд

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + x_2y_2}{e(1 + dx_1x_2y_1y_2)}, \frac{y_1y_2 - x_1x_2}{e(1 - dx_1x_2y_1y_2)}\right) \tag{2.12}$$

закон подвоєння для співпадаючих точок, відповідно, записується так

$$2(x_1, y_1) = \left(\frac{2x_1 y_1}{e(1 + d{x_1}^2 {y_1}^2)}, \frac{{y_1}^2 - {x_1}^2}{e(1 - d{x_1}^2 {y_1}^2)} \right). \tag{2.13}$$

Принциповими відмінностями 2.11 від 2.1 є циклічна структура групи точок (у відношенні точок 2-го порядку) і відсутність особливих точок (з діленням на 0 в законі додавання)ю Остання властивість названа як "повнота закону додавання". Так і для кривої 2.1, зворотня точка означена як $-(x_1, y_1) = (-x^1, y_1)$, нулем групи точок (нейтральним елементом аддитивної групи точок) тут є очка $O = (0, e)$, але існує лише єдина точка 2-го порядку $D = (e, -e)$ і рівно 2 точки 4-го порядку $\pm F = (\pm e, 0)$.

2.3 Властивості еліптичних кривих в формі Едвардса

Завдяки таким властивостям[1], як рекордна швидкість, можливість представлення нейтрального елемента в афінних координатах, універсальність закону додавання, еліптичні криві в формі Едвардса наразі є найбільш швидкими та перспективними для використання в асиметричних криптосистемах.

Симетрія рівнянь кривих Едвардса відносно обох координат тягне за собою корисні особливості цих кривих. Виключаючи неактуальні ізоморфні криві, в кривих Едвардса достатньо використовувати лише одина параметр d замість двох звичайних a и b класичної кривої в канонічній формі Вейєрштрасса.

В роботі [4] автори узагальнили і розширили клас кривих Едвардса додаванням нового параметра a. Вони назвали цей клас скрученими кривими Едвардса. Надалі прогрес в дослідженні властивостей цього класу скручених кривиxx отримано в роботі [4], в якій знайдено

альтернативні формули для закону додавання точок кривої, означені основні особливості точок для закону і запропоновано метод розрахунку координат суми точок в розширених проективних координатах.

В роботі [4] були приведені необхідні та достатні умови того, що еліптична крива, що задана в канонічній формі, є ізоморфною деякій кривій Едвардса. На основі цих критеріїв було знайдено точне число кривих Едвардса над будь-яким скінченним полем в залежності від його характеристики.

У роботі [2] сформульовані і обґрунтовані критерії подільності точки кривої Едвардса на довільне натуральне число.

На їх основі розроблені алгоритми отримання кореня довільної степені із точки кривої, або в термінах адитивної групи алгоритми знаходження точки ділення на довільне натуральне число. У цій статті виконано детальний порівняльний аналіз нових і класичного алгоритмів обчислення базової точки кривої; показано, що запропоновані далі алгоритми мають виграш в швидкодії в сотні разів. Зауважимо, що цей виграш збільшується з ростом характеристики простого поля, над яким побудована крива.

Приведені критерії подільності і алгоритми отримання кореня в групі точок еліптичної кривої є схожими на аналогічні критерії, отримані в [4] для простих полів і скінченних кілець. Але для еліптичних кривих ці алгоритми мають набагато більше прикладне значення.

2.4 Перетворення еліптичної кривих в формі Едвардса в форму Вейєрштрасса

Канонічна форма еліптичної кривої над скінченним полем F_q має вигляд

$$v^2 = u^3 + au + b, a, b \in F_q \tag{2.14}$$

Ізоморфізм між кривими в формі Вейєрштрасса і Едвардса може забеспечити не будь-яка пара параметрів a,b. Необхідною і достатньою умовою ізоморфізму є існування на кривій рівно двох точок 4-го порядку.

В роботі [4] розглянуто криву в формі

$$v^2 = (u - 1 - e^4 d)(u^2 - 4e^2 d) \tag{2.15}$$

Одразу зазначимо, що парабола $(u^2 - 4e^4 d)$ в правій частині рівняння не має коренів в полі F_q в силу неквадратичності параметру d, тому крива має єдину точку 2-го порядку $(1 + e^4 d, 0)$.

Раціональна заміна змінних

$$u = \frac{-2e(w - e)}{x^2}, v = \frac{4e^2(w - e) + 2ex^2(e^4 d + 1)}{x^3}, w = (e^2 dx^2 - 1)y, \tag{2.16}$$

трансформує криву в формі Едвардса з модифікацією Бернстейна-Ланге в форму Вейєрштрасса.

2.5 Перетворення кривої в формі Вейєрштрасса в форму Монтгомері

В роботах [2,4] надано детальний аналіз параметрів a, b кривої

$$v^2 = u^3 + au + b, a, b \in F_q. \tag{2.17}$$

що породжують ізоморфні криві в формі Монтгомері і Едвардса.

Рівняння еліптичної кривої в формі Монтгомері має вигляд:

$$v^2 = y^3 + Au^2 + Gu, A < G \in F_q \tag{2.18}$$

Нехай c - єдиний корінь кубічного поліному в правій частині рівняння 2.17. Тоді це рівняння можна переписати у вигляді

$$Y^2 = (X - c)(x^2 + cX + a + c^2), b = -c(a + c^2). \tag{2.19}$$

Із рівності $c^3 + ac + b = 0$ в цьому рівнянні випливає, що c - корінь кубічного поліному. Заміною $X - c \to u, Y \to v$ отримуємо рівняння в формі Монтгомері, в якому

$$v^2 = u^3 + 3cu^2 + (a + 3c^2)u \to A = 3c, G = (a + 3c^2), \tag{2.20}$$

Далі замість пари параметрів a, b нам буде зручно використовувати параметри a, c, і при цьому $b = -c(a + c^2)$.

Покладемо умови, що накладаються на параметри a, c, - при яких мається єдина точка 2-го порядку і рівно 2 точки 4-го порядку. Другою задачею є знаходження залежностей між параметрами a і c канонічної форми еліптичної кривої і параметром d кривої $x^2 + y^2 = 1 + dx^2y^2$ в формі Едвардса.

Необхідними і достатніми умовами існування єдиної точки 2-го і двох

точок 4-го порядку кривої є:

$$\left(\frac{-(3c^2+4a)}{p}\right) = -1, \left(\frac{(3c^2+4a)}{p}\right) = 1 \tag{2.21}$$

В ході доведення отримані квадрати для координат 4-го порядку

$$u_1^2 = 3c^2 + a = \delta, v_1^2 = u_1^2(2u_1 + 3c) \tag{2.22}$$

Звідси випливає, що параметр G повинен бути квадратом, або

$$\left(\frac{\delta}{p}\right) = \left(\frac{(3c^2+a)}{p}\right) = 1 \tag{2.23}$$

З останнього виразу 2.22 можна отримати

$$3c = \frac{v_1^2}{u_1^3}\left(1 - 2\frac{u_1^3}{v_1^2}\right)u_1 = 2\frac{1+d}{1-d}u_1.d = 1 - 4\frac{u_1^3}{v_1^2} \tag{2.24}$$

Перша формула в 2.24 дозволяє виразити параметр d через параметри a, c канонічної форми кривої

$$d = \frac{3c - 2u_1}{3c + 2u_1} \tag{2.25}$$

З врахуванням 2.22, 2.24 коефіцієнти дорівнюють:

$$A = 3c = 2\frac{1+d}{1-d}u_1, G = (a + 3c^2) = u_1^2. \tag{2.26}$$

Тоді це рівняння приймає вигляд

$$v^2 = u^3 + 2\frac{1+d}{1-d}u_1u^2 + u_1^2u. \tag{2.27}$$

Заміною $v^2 \to \frac{1}{1-d}v^2$, діленням правої частини на u_1^3 і заміною $\frac{u}{u_1} \to u$ рівняння 2.20 в формі Монтгомері тепер може бути приведено до вигляду, який залежить лише від одного параметра d

$$\frac{1}{1-d}v^2 = u^3 + 2\frac{1+d}{1-d}u^2 + u. \tag{2.28}$$

Якщо ліву частину цього рівняння помножити на квадратичний нелишок d, то відповідні розв'язки (точки кривої) перетворюються в "нерозв'язки"(дири) і навпаки. Це справедливо для всіх точок, крім точок 2-го порядку, що зберігають свої $u-$координати. Тоді отримуємо рівняння для кривої квардатичного кручення

$$\frac{d}{1-d}v^2 = u^2 + 2\frac{1+d}{1-d}u^2 + u. \tag{2.29}$$

Пари кривих 2.28, 2.29 ще називають парами кривих кручення. Перехід від одної з кривих до іншої виконується простою заміною $d \to d^{-1}$.

Дійсно рівняння 2.28 після такої заміни має вигляд

$$\frac{d}{1-d}v^2 = u^3 + 2\frac{1+d}{1-d}u^2 + u. \tag{2.30}$$

Тоді підставляючи $(-u) \to u$, отримаємо рівняння 2.29. Якщо порядок кривої 2.28 дорівнює $N_E = q + 1 - t$, то порядок кривої кручення $N_E^t = q + 1 + t$, (де $t-$ слід рівняння Фробеніуса) симетричний відносно середнього значення $q + 1$.

Зазначимо, що для кривих Едвардса порядок кривої $N_E = 0 mod 4$, тому слід рівняння Фробеніуса t може дорівнювати 0 лише для значення модуля $p = 3 mod 4$. В такому випадку елемент поля (-1) є квадратичним нелишком, і при значення $d = d^{-1} = -1$ пара кривих кручення вироджується в одну суперсингулярну криву з порядком $N_E = q + 1$.

Обмеження параметра d. Так як $u_1 \neq 0, d \neq 1$. Якщо допустити, що $d = 0$, то в рівнянні 2.28 отримуються кратні корені кубіки, тобто порушується несингулярність кривої. Вимоги єдиності точки другого порядку еквівалентна тому, що дискримінант правої частини рівняння 2.28 або 2.29 після отримання кореня $u = 0$ повинен бути нелишком.

$$\Delta = 4\left(\left(\frac{1+d}{1-d}\right)^2 - 1\right) = \frac{16d}{1-d^2} \neq C^2 \Rightarrow \left(\frac{d}{p}\right) = -1. \tag{2.31}$$

Звідси випливає, що $d-$ квадратичний нелишок в полі F_q

Форма кривої 2.28 за допомогою нескладної заміни $(u, v) \to (x, y)$ придовиться до ізоморфної кривої в формі Едвардса.

2.6 Необхідні та достатні умови ізоморфізму між еліптичними кривими в формі Вейєрштрасса та еліптичними кривими в формі Едвардса

Циклічні еліптичні криві Едвардса завжди мають одну точку 2-го порядку і дві точки 4-го порядку. Тобто еліптична крива в канонічній формі ізоморфна еліптичній кривій в фомі Едвардса в тому і тільки тому випадку, якщо вона має рівно дві точки четвертого порядку.Кривих в канонічній формі $y^2 = x^3 + ax + b$ з такою властивістю порівняно мало, тому для побудови ізоморфним їм кривим Едвардса виникає задача пошуку кривих в формі Вейєрштрасса з двома точками 4-го порядку.

2.6.1 Необхідні і достатні умови існування рівно двох точок четвертого порядку для еліптичної кривої в формі Вейєрштрасса

Розглянемо криву в канонічній формі над полем характеристики $p > 3$:

$$E_p : y^2 = x^3 + ax + b, \tag{2.32}$$

де $4a^3 + 27b^2 \neq 0$, $a, b \in F_p$.

Згідно з означенням, операція подвоєння точки $P = (x_1, y_1)$, яка дає дві координати точки $2P = (x_3, y_3)$, задається наступним чином:

$$\begin{cases} x_3 = v^2 - 2x_1, \\ y_3 = -y_1 - v(x_3 - x_1), \quad v = \frac{3x_1^2 + a}{2y_1} \end{cases} \tag{2.33}$$

В подальшому нам знадобляться наступні стандартні позначення. Множина приведених квадратичних лишків за модулем простого числа p будемо позначати Q_p:

$$Q_p = \left\{ x \in F_p \middle| \left(\frac{x}{p}\right) = 1 \right\}, \tag{2.34}$$

Розглянемо криві 2.32, порядок яких ділиться на 2. В цьому випадку крива обов'язково має точку другого порядку (це буде випливати з теореми Силова). Згідно 2.33, точка $P = (x_1, y_1)$ буде точкою другого порядку тоді і тільки тоді, коли $y_1 = 0$ (в цьому випадку при обчисленні точки $2P$ в 2.33 виникає ділення на 0), тобто точка другого порядку буде мати координати $(c, 0)$, для деякого cF_p. Підставляючи в рівняння кривої 2.32 значення $y = 0$, отримуємо, що корінь c - корінь рівняння $x^3 + ax + b = 0$ в полі F_p (який обов'язково існує, згідно з існуванням точки другого порядку). Тоді в наших позначеннях рівняння 2.32 можна переписати в вигляді

$$y^2 = (x - c)(x^2 + cx + a + c^2), \tag{2.35}$$

де $b = -c^3 - ac$, $c \in F_p$.

Як згадувалось раніше, еліптична крива в канонічній формі ізоморфна еліптичній кривій в фомі Едвардса в тому і тільки тому випадку, якщо вона має рівно дві точки четвертого порядку. Наступна теорема дає необхідні та достатні умови (в термінах параметрів еліптичної кривої в формі Вейєрштрасса 2.32) існування на еліптичній кривій E_p рівно двох таких точок.

Теорема 2.1. *Необхідною і достатньою умовою існування рівно двох точок четвертого порядку на кривій E_p є одночасне виконання наступних двох рівнянь:*

$$1)\ \left(\frac{-(3c^2+4a)}{p}\right) = -1, \qquad 2)\ \frac{\delta}{p} = 1,\ \text{де } \delta = 3c^2 + a \tag{2.36}$$

Доведення. Доведемо необхідність даних умов. Нехай крива має дві точки четвертого порядку, покажемо, що при цьому виконуються 2.36. Очевидно, вона не може мати більше однієї точки другого порядку (так як, згідно з означенням порядку точки кривої, сума точок четвертого і другого порядку буде точкою четвертого порядку). З цього випливає, що парабола в правій частині 2.35 не має коренів в F_p, тобто дискримінант відповідного квадратного рівняння є квадратичним нелишком. цей дискримінант дорівнює

$$c^2 - 4(a + c^2) = -(3c^2 + 4a);$$

і оскільки він квадратичний нелишок, то

$$\left(\frac{-(3c^2+4a)}{p}\right) = -1.$$

Необхідність першої умови в 2.36 доведена.

Зауважимо, що умова $3(c^2+4a) \neq 0$, яке випливає з пукту 1) формули 2.36, виключає кратні корні кубічного рівняння і, тим самим, сингулярні криві з дискримінантом $\Delta = 0$ [8].

Нехай $P = (x_1, y_1)$ - точка 4-го порядку. Тоді при її подвоєнні, згідно 2.33, отримуємо точку другого порядку $D = (c, 0)$:

$$\begin{cases} \left(\frac{3x_1^2+a}{2y_1}\right)^2 - 2x_1 = c; \\ -y_1 - \left(\frac{3x_1^2+a}{2y_1}\right)(c - x_1) = 0. \end{cases} \tag{2.37}$$

З першого рівняння цієї системи отримуємо вираз

$$y_1^2 = \frac{(3x_1^2 + a)^2}{4(c + 2x_1)}$$

а з другого рівняння цієї системи отримуємо вираз

$$y_1^2 = -\frac{(3x_1^2 + a)(c - x_1)}{2}$$

Прирівнюючи праві частини цих виразів і скорочуючи на множник $3x_1^2 + a$, отримаємо квадратне рівняння для координати x_1 цієї точки:

$$x_1^2 - 2cx_1 - (2c^2 + a) = 0. \tag{2.38}$$

Корні цього рівняння існують (внаслідок існування точки 4-го порядку), з цього випливає, що дискримінант δ цього рівняння або дорівнює нулю, або є квадратичним лишком. Якщо дискримінант дорівнює нулю, то, при $y = 0$, рівняння 2.35 приймає вигляд:

$$(x - c)^2(x + 2c) = 0,$$

внаслідок чого, на кривій існують дві точки другого порядку. Але тоді безпосереднім обчисленням отримуємо, що сума будь-якої такої точки з точкою четвертого порядку також буде точкою четвертого порядку, що суперечить припущенню теореми про існування рівно двої точок четвертого порядку. З цього випливає, що дискримінант δ є квадратичним лишком. Тобто виконується умова 2) формули 2.36. Необхідність умови 2.36 доведена.

Доведемо достатність.

Нехай виконуються умови 2.36. Покажемо, що при цьому існує рівно два розв'язки системи 2.37. Шляхом перетворень рівнянь даної системи отримаємо рівняння 2.38 з однією змінною x_1. Оскільки виконується умова 1) формули 2.36, то існує два корені даного рівняння:

$$x_1^{(1),(2)} = c \pm \sqrt{\delta} = c \pm \sqrt{3c^2 + a} \tag{2.39}$$

Підставляючи ці вирази в друге рівняння системи 2.37, отримуємо:

$$y_1^2 = -2^{-1}(3(c \pm \sqrt{\delta})^2 + a)(\mp\sqrt{\delta}) = \pm 2^{-1}\sqrt{\delta}(3c^2 \pm 3c\sqrt{\delta} + 3\delta + a) =$$

$$= \pm 2^{-1}\sqrt{\delta}(3c^2 \pm 6c\sqrt{\delta} + 3\delta + a) = \pm 2^{-1}\sqrt{\delta}(\pm 6c\sqrt{\delta} + 4\delta) = \qquad (2.40)$$

$$= \pm\sqrt{\delta}(\pm 3c\sqrt{\delta} + 2\delta) = \pm\delta(\pm 3c + 2\sqrt{\delta}) = \delta(3c \pm 2\sqrt{\delta})$$

З 2.40 випливає, що розв'язок системи 2.37 існує тоді і тільки тоді, коли хоча б один з виразів

$$1) 3c - 2\sqrt{\delta}$$

$$2) 3c + 2\sqrt{\delta} \qquad (2.41)$$

є квадратичним лишком (так як, за умовою, $\left(\frac{\delta}{p}\right) = 1$).

Покажемо, що в нашому випадку рівно один з виразів 2.41 буде квадратичним лишком.

Дійсно, перемноживши ці вирази, ми отримаємо

$$(3c - 2\sqrt{\delta})(3c + 2\sqrt{\delta}) = 9c^2 - 4\delta = -(3c^2 + 4a),$$

що згідно пуктну 1) умови 2.36, є квадратичним нелишком. Звідси, внаслідок властивості мультиплікативності символу Лежандра, випривається, що рівно один з виразів 2.41 є квадратичним лишком.

Якщо $3c - 2\sqrt{\delta}$ є квадратичним лишком, то існують

$$y_1^{(1),(2)} = \pm\sqrt{\delta(3c + 2\sqrt{\delta})};$$

в інакшому випадку існують

$$y_1^{(1),(2)} = \pm\sqrt{\delta(3c - 2\sqrt{\delta})};$$

і тоді або пари

$$\left(3c - 2\sqrt{\delta}, \pm\sqrt{\delta(3c + 2\sqrt{\delta})}\right),$$

або пари

$$\left(3c - 2\sqrt{\delta}, \pm\sqrt{\delta(3c - 2\sqrt{\delta})}\right),$$

відповідно, є двома розв'язками системи 2.37. Прямою перевіркою (підстановкою в рівняння 2.32 або в рівняння 2.35) впевнюємось, що ці пари є розв'язками рівнянь 2.32 і 2.35, відповідно, кожна пара задає координати деякої точки даної кривої. Внаслідок виконання 2.37, кожна з двох отриманих точок є точкою 4-го порядку. Інших розв'язків система 2.37 не має, з чого випливає, що на кривій 2.32 існує рівно дві точки четвертого порядку, що і доводить достатність умов 2.36.

Варто відмітити, що криві з нульовими значеннями параметрів a або b мають погані криптографічні властивості і не використовуються в криптографічних застосунках [7]. Теорема доведена. □

2.7 Повні еліптичні криві Едвардса над простим полем

Клас повних еліптичних кривих Едвардса над простим полем володіє наступними властивостями. В порівнянні з кривими в формі Вейєрштрасса вони виграють в швидкодії арифметики експоненціювання точки кривої на 50-60% [1,2]. При цьому повні криві мають афінні координати нейтральної точки групи і універсальність закону додавання, що ще більше пришвидшує реалізацію криптоалгоритмів.

Симметрія точок кривих Едвардса відносно обох координатних осей тягне за собою наступні властивості. Виключаючи з розгляду ізоморфні криві, в кривих Едвардса достатньо використовувати один параметр d замість двох параметрів a, b кривої в канонічній формі Вейєрштрасса.

Повні криві Едвардса були описані в роботі [1]. Рівняння 2.11 при $e = 1$ з точністю до ізоморфізму задає повну криву Едвардса вигляду

$$E : x^2 + y^2 = 1 + dx^2y^2, d(1-d) \neq 0, \left(\frac{d}{p}\right) = -1, \tag{2.42}$$

де параметр d - квадратичний нелишок. В інтересах криптографічних застосунків використовуються прості поля F_p, хоча можуть використовуватись і розширені поля F_p^m, характеристики $p \neq 2$.

Універсальний закон додавання двох точок кривої 2.42 має вигляд

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1x_2 - y_1y_2}{1 - dx_1x_2y_1y_2}, \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}\right) \tag{2.43}$$

Закон подвоєння точки (x_1, y_1), записується так:

$$2(x_1, y_1) = \left(\frac{x_1^2 - y_1^2}{1 - dx_1^2y_1^2}, \frac{2x_1y_1}{1 + dx_1^2y_1^2}\right) \tag{2.44}$$

Нагадаємо, що вираш законів 2.43 та 2.44 - горизонтальна симетрія зворотних точок, при цьому $-P = -(x_1, y_1) = (x_1, -y_1)$. Нейтральний елемент групи тепер дорівнює $O = (1, 0)$, точка $D = (-1, 0)$ - точка другого порядку та $\pm F = (0, \pm 1)$ - точки 4-го порядку.

Серед загальносистемних параметрів криптосистеми на еліптичних кривих найважливішим є її геренатор як точка достатньо великого простого порядку n. При використовуванні кривих Едвардса над простим полем порядок кривої $N_E = 4n$, де n - велике просте число. Після знаходження випадкової точки $Q = (x_Q, y_Q)$ кривої генератор криптосистеми порядка n можна знайти як точку $G = (x_G, y_G) = 4Q$, для цього потрібно два подвоєння точки (тобто дві групові операції).

2.8 Скручені еліптичні криві Едвардса

В роботі [1] скручені криві Едвардса (twisted Edwards curves) були означені як узагальнення кривих Едвардса $x^2 + y^2 = 1 + dx^2y^2$ шляхом введення нового параметра a в рівняння без обмежень на квадратичність параметрів a та d.

$$ax^2 + y^2 = 1 + dx^2y^2, a \neq d, a, d \in F_q^*, d \neq 1, p \neq 2. \tag{2.45}$$

Таке означення неможна признати коректним, так як воно породжує три різних класи, що не перетинаються, кривих з різними властивостями при цьому два з цих класів ізоморфні кривим з параметром $a = 1$. Введення нового параметра $a \neq 1$ не дає такого ізоморфізму в єдиному випадку, коли обидва параметри не є квадратами:

$$\left(\frac{a}{p}\right) = -1, \left(\frac{d}{p}\right) = -1 \tag{2.46}$$

Саме такий випадок і визначає окремий клас скручених кривих Едвардса. На яких можна використовувати модифіковані закони подвоєння і додавання точок, які забезпечують збереження загальноприйнятої горизонтальної симетрії зворотних точок. Всі криві Едвардса, що поєднують різні класи кривих, що не перетинаються, означаються кривими в узагальненій формі Едвардса з рівнянням:

$$E_{a,d} : x_a^2y^2 = 1 + dx^2y^2, a \neq d, a, d \in F_q^*, d \neq 1, p \neq 2. \tag{2.47}$$

Окремим випадком таких кривих є скручена крива Едвардса з обмеженнями на параметри a та d.

$$E_{a,d} : x_a^2 y^2 = 1 + dx^2 y^2, a \neq d, a, d \in F_q^*, d \neq 1, \left(\frac{a}{p}\right) = -1, \left(\frac{d}{p}\right) = -1. \tag{2.48}$$

Модифіковані закони додавання і подвоєння точок кривої 2.48 мають наступний вигляд:

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1 x_2 - a y_1 y_2}{1 - d x_1 x_2 y_1 y_2}, \frac{x_1 y_2 + y_1 x_2}{1 + d x_1 x_2 y_1 y_2}\right). \tag{2.49}$$

$$2(x_1, y_1) = \left(\frac{x_1^2 - a y_1^2}{1 - d x_1^2 y_1^2}, \frac{2 x_1 x_2}{1 + d x_1^2 y_1^2}\right). \tag{2.50}$$

При $y = 0$ в 2.48 отримаємо $x_{1,2} = \pm 1$. На осі x лежать 2 точки: нейтральний елемент групи $O = (1, 0)$ і точка $D_0 = (-1, 0)$ 2-го порядку. При $x = 0$ в 2.48 отримаємо $y_{1,2} = \pm\frac{1}{\sqrt{a}}$. Таким чином, в силу неквадратичності параметра a точки 4-го порядку $\pm F_0 = (0, \pm\frac{1}{\sqrt{a}})$ на кривій 2.48 не існують.

2.9 Альтернативний закон додавання точок

В статті [7] вперше було показано альтернативні формули для закону додавання точок скрученої еліптичної кривої Едвардса, в якому виразивши параметри a та d через координати точок, було отримано наступну формулу:

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1 y_1 + x_2 y_2}{y_1 y_2 + a x_1 x_2}, \frac{x_1 y_1 - x_2 y_2}{x_1 y_2 + x_2 y_1}\right). \tag{2.51}$$

Його особливістю є незалежність координат від обох параметрів a та b кривої 2.48. Зауважимо, що цей закон не працює з подвоєнням точки, так як на другій координаті виникає невизначеність $0/0$. Тому при

подвоєнні точок доводеться повертатись до звичайної формули 2.50. Тут основна проблема пов'язана з постійними переходами до різних проективних координат. Хоча альтернативний закон 2.51 в загальному випадку не є повним, для точок непарного порядку особливих точок немає і формули 2.51 є конструктивними.

Теорема 2.2. *Нехай маємо скручену криву Едвардса $E_{a,d}$ 2.48. Для фіксованої точки кривої $P = (x_1, y_1)$ знайдеться така точка $Q = (x_2, y_2)$, для якої:*

1) $y_1y_2 + ax_1x_2 = 0$ *тоді і тільки тоді, коли* $Q \in S_x$, *де*

$$S_x = \{\left(\frac{y_1}{\sqrt{a}}, -x_1\sqrt{a}\right), \left(-\frac{y_1}{\sqrt{a}}, -x_1\sqrt{a}\right), \left(\frac{1}{x_1\sqrt{ad}}, -\frac{\sqrt{a}}{y_1\sqrt{d}}\right)\left(\frac{-1}{x_1\sqrt{ad}}, \frac{\sqrt{a}}{y_1\sqrt{d}}\right)\};$$

2) $x_1y_2 - y_1x_2 = 0$ *тоді і тільки тоді, коли* $Q \in S_y$, *де*

$$S_y = \{(x_1, y_1), (-x_1, -y_1), \left(\frac{1}{y_1\sqrt{d}}, \frac{\sqrt{1}}{x_1\sqrt{d}}\right)\left(\frac{-1}{y_1\sqrt{d}}, \frac{\sqrt{-1}}{x_1\sqrt{d}}\right)\};$$

Розглянемо випадок $\left(\frac{a}{p}\right) = 1, \left(\frac{d}{p}\right) = -1$. Тоді в кожному з множин S_x, S_y залишається по дві перших точки. Їх координати для множини S_x виглядаються як $Q = P \pm F$, де $\pm F = \left(\pm\frac{1}{\sqrt{a}}, 0\right)$- точки 4-го порядку. Тоді виникає особливість при $Q + P = 2P \pm F$. Координати точод для множини S_x виглядають як $Q = P$ та $Q = P + D$, де $D = (0, 1)$- точка 2-го порядку. Тут особливість виникає при $Q+P = 2P$ і при $Q+P = 2P+D$. Всі особливі випадки породжуються подвоєнням точки P з можливим додаванням з ним точок 4-го або 2-го порядку.

Якщо $P-$ точка непарного порядку n, то $Ord(2P) = n$, так як $n2P = O$. Звідси випливає, що $Ord(2P \pm F) = 4n$ і $Ord(2P + D) = 2n$. Другими словами, особливості в розгляненому випадку можуть виникати лише при додаванні різних точок парних порядків . При обчисленні скалярного множення kP при великих значеннях k для коїної точки P великого порядку може існувати лише 3 точки Q таких, що сума $Q + P$ не визначена, а така подія малоімовірна. В криптосистемі з генератором G простого порядку n додавання будь-яких різних точок з групи $< G >$ особливостей не породжує. Це завжди справедливо для всіх точок непарного порядку.

Висновки до розділу 2

В цьому розділі розглянуто еліптичні криві в формі Едвардса, надано їх математичний опис, наведено операції на цих кривих і показано за рахунок яких властивостей операції на таких кривих є більш швидкими ніж на кривих в формі Вейєрштрасса.

3 ПЕРЕТВОРЕННЯ ЕЛІПТИЧНОЇ КРИВОЇ У ФОРМІ МОНТГОМЕРІ В ЕЛІПТИЧНУ КРИВУ В ФОРМІ ЕДВАРДСА

В цьому розділі описуються необхідні та достатні умови існування кривої у формі Едвардса, що є ізоморфною до заданої кривої у формі Монтгомері. Наведено формулювання теореми, на основі отриманих умов та її строге доведення. Наведено формулювання теореми, що показує кількість еліптичних кривих у формі Монтгомері, які є ізоморфними повним еліптичним кривим в формі Едвардса та її строге доведення. Описується алгоритм, що виконує ізоморфне перетворення (при виконанні умов ізоморфізму) кривої у формі Монтгомері у криву в формі Едвардса.

3.1 Необхідні та достатні умови ізоморфізму між еліптичними кривими в формі Монтгомері та еліптичними кривими в формі Едвардса

Нехай еліптична крива над скінченним полем F_q задана у формі Монтгомері.

$$M : v^2 = u^3 + Au^2 + Gu. \tag{3.1}$$

Тоді справедливою є наступна теорема:

Теорема 3.1. *Еліптична крива в формі Монтгомері 3.1 ізоморфна деякій повній еліптичній кривій в формі Едвардса тоді і тільки тоді, коли виконуються умови*

$$\left(\frac{G}{p}\right) = 1; \left(\frac{A^2 - 4G}{p}\right) = -1. \tag{3.2}$$

Доведення. Будь-яка еліптична крива у формі Монтгомері 3.1 може бути отримана з еліптичної кривої у формі Вейєрштрасса

$$y^2 = x^3 + ax + b \tag{3.3}$$

тоді й тільки тоді, коли права частина рівності 3.3 має корінь c, тобто $\exists c \in \mathrm{F}_p$: $x^3 + ax + b = (x - c)(x^2 + cx + a + c^2)$. Тоді заміною

$$u = x - c; A = 3c; G = a + 3c^2 \tag{3.4}$$

з рівності 3.3 отримаємо 3.1.

Як відомо з [2], крива 3.3 буде ізоморфною деякій повній кривій Едвардса тоді і тільки тоді, коли виконуються одночасно такі умови:

$$\left(\frac{-(3c^2 + 4a)}{p}\right) = -1; \left(\frac{3c^2 + a}{p}\right) = 1. \tag{3.5}$$

Використовуючи 3.4, вираз $-(3c^2 + 4a)$ можна переписати як

$$-(3c^2 + 4a) = -(4G - 9c^2) = -(4G - A^2) = A^2 - 4G. \tag{3.6}$$

Тоді, з використанням 3.4 і 3.6, умови 3.5 можуть бути записані наступним чином:

$$\left(\frac{A^2 - 4G}{p}\right) = -1; \left(\frac{G}{p}\right) = 1. \tag{3.7}$$

Теорема доведена. □

З теореми 3.2 випливає наступний наслідок.

Наслідок 3.1. *Нехай для еліптичної кривої 3.1 виконуються умови 3.5. Позначимо $u_1, u_2 \in E_p^*$- корені з G за модулем p, $u_2 = p - u_1$. Тоді виконується рівно одна з наступних умов:*

$$2u_1 + 3c \in Q_p \text{ або } 2u_2 + 3c \in Q_p \tag{3.8}$$

Доведення.

Перемножимо обидва вирази у 3.8:

$(2u_1 + 3c)(2u_2 + 3c) = (3c + 2u_1)(3c - 2u_1) = 9c^2 - 4u_1^2 = A^2 - 4G$

За першою умовою з 3.5, $A^2 - 4G \in Q_p$.

Тому, оскільки $A^2 - 4G = (3c + 2u_1)(3c - 2u_1)$, вирази $3c + 2u_1$ та $3c - 2u_1$ не можуть бути обидва квадратичними лишками або обидва квадратичними нелишками, оскільки у цьому випадку їх добуток буде квадратичним лишком. Отже, рівно один з виразів $3c \pm 2u_1$ є квадратичним лишком.

Наслідок доведено. □

З використанням цього наслідку, а також згідно [2], отримаємо такий алгоритм, що переводить криву у формі Монтгомері в форму Едвардса.

3.2 Алгоритм перетворення кривої у формі Монтгомері в еліптичну криву в формі Едвардса.

Отримані результати дозволяють побудувати наступний алгоритм побудови еліптичних кривих у формі Едвардса з еліптичних кривих в формі Монтгомері.

Алгоритм 3.1

Відображення кривої у формі Монтгомері у криву в формі Едвардса.

Вхід: A, G - параметри еліптичної кривої в формі Монтгомері 3.1.

Вихід: Параметри повної еліптичної кривої в формі Едвардса.

1) Перевірити виконання умов: $\left(\frac{A^2-4G}{p}\right) = -1; \left(\frac{G}{p}\right) = 1.$

Якщо умови не виконуються, то повернути "крива не ізоморфна кривій Едвардса"; зупинити роботу алгоритму.

2) Обчислити u_1 - довільний корінь з G за $modp$.

Якщо $2u_1 + 3c \notin Q_p$, то $u_1 \leftarrow p - u_1$.

3) Обчислити

$$d = (3c - 2u_1)(3c + 2u_1)^{-1} modp \tag{3.9}$$

4) Вивести рівняння повної еліптичної кривої в формі Едвардса

$$x^2 + y^2 = 1 + dx^2y^2. \tag{3.10}$$

Доведення. Коректність роботи алгоритму

Згідно наслідку 1, після завершення кроку 2 ми отримаємо таке значення u_1, що $2u_1 - 3c \notin Q_p$.

Покажемо, що вираз 3.9 дійсно дає квадратичний нелишок. Перепишемо 3.9 у такому вигляді

$$d = \frac{3c - 2u_1}{3c + 2u_1} = \frac{(3c - 2u_1)(3c + 2u_1)}{(3c + 2u_1)^2}. \tag{3.11}$$

У вигляді 3.11 знаменник є квадратом, отже, він є квадратичним лишком. Чисельник, згідно з наслідком 1, є квадратичним нелишком. Тому $d \notin Q_p$ і крива 3.11 дійсно є повною.

Коректність доведено.

□

Час роботи алгоритму

1) Обчислення символу лежандра: $O((\log p)^3)$;

2) Обчислення u_1: множення та додавання за $\bmod p$, що не перевищують p, виконуються за $O((\log p)^2)$;

3) Обчислення d: множення та додавання за $\bmod p$, що не перевищують p, виконуються за $O((\log p)^2)$, крім того, для заходження оберненого за модулем числа використовується розширений алгоритм Евкліда, для якого час роботи $O((\log p)^3)$;

Отже, загальний час роботи алгоритму можна оцінити як $O((\log p)^3)$.

3.3 Кількість кривих в формі Монтгомері, які є ізоморфними повним кривим в формі Едвардса

Тепер потрібно дати відповідь на питання: скільки існує таких пар $(A, G) \in Z_p \times Z_p$, що рівняння 3.1 задає криву, ізоморфну деякій повній кривій Едвардса?

Відповідь на це питання дає наступна теорема.

Теорема 3.2. *Нехай $N_{M\to E}$ - кількість еліптичних кривих у формі Монтгомері, які є ізоморфними повним еліптичним кривим в формі Едвардса. Тоді*

1) Якщо $p \equiv 1(mod 4)$, то $N_{M\to E} = \frac{p-1}{4}$;

2) Якщо $p \equiv 3(mod 4)$, то $N_{M\to E} = \frac{p-3}{4}$;

Доведення. Для доведення нам необхідні результати роботи [9], а саме подначення та лема Гауса про характери пар елементів простого скінченного поля і її наслідки.

Для зручності, наведемо їх формулювання:

Для довільного $l \in N, 1 \nleq l \nleq p-1$, введемо наступні множини

$$rr_l = \left\{(i, i+l) mod p | (i \in Z_p^*\{p-l\} \wedge \left(\left(\frac{i}{p}\right) = \left(\frac{i+l}{p}\right) = 1\right)\right\}$$

$$rn_l = \left\{(i, i+l) mod p | (i \in Z_p^*\{p-l\} \wedge \left(\left(\frac{i}{p}\right) = 1, \left(\frac{i+l}{p}\right) = -1\right)\right\}$$

$$rn_l = \left\{(i, i+l) mod p | (i \in Z_p^*\{p-l\} \wedge \left(\left(\frac{i}{p}\right) = -1, \left(\frac{i+l}{p}\right) = 1\right)\right\}$$

$$rr_l = \left\{(i, i+l) mod p | (i \in Z_p^*\{p-l\} \wedge \left(\left(\frac{i}{p}\right) = \left(\frac{i+l}{p}\right) = -1\right)\right\}$$

Лема 3.1. *Нехай p - просте число, $l \in Z_p^*$. Тоді справедливі наступні рівності:*

$$rn_l + nn_l = \frac{p-2+\left(\frac{l}{p}\right)}{2};$$

$$rr_l + nr_l = \frac{p-2-\left(\frac{l}{p}\right)}{2};$$

$$nr_l + nn_l = \frac{p-2+\left(\frac{-l}{p}\right)}{2};$$

Наслідок 3.2. *Позначимо* $\epsilon_1 = \left(\frac{l}{p}\right)$ *та* $\epsilon_1 = \left(\frac{-l}{p}\right)$. *Тоді справедливі наступні твердження:*

$$rn_l = \frac{p-1+\epsilon_1-\epsilon_2}{4};$$

$$nn_l = \frac{p-3+\epsilon_1+\epsilon_2}{4};$$

$$rr_l = \frac{p-3-\epsilon_1-\epsilon_2}{4};$$

$$nr_l = \frac{p-1-\epsilon_1+\epsilon_2}{4};$$

Наслідок 3.3. *Для довільного простого* p *позначимо* $Q_p = \{x \in Z_p^* | \exists y \in Z : x \equiv y^2 (mod p)\}$. *Тоді якщо* $l \in Q_p$, *то*

$$rn_l = \frac{p-\left(\frac{-1}{p}\right)}{4};$$

$$nn_l = \frac{p-2+\left(\frac{-1}{p}\right)}{4};$$

$$rr_l = \frac{p-4-\left(\frac{-1}{p}\right)}{4};$$

$$nr_l = \frac{p-2+\left(\frac{-1}{p}\right)}{4};$$

В протилежному випадку (коли $l \notin Q_p$*):*

$$rn_l = \frac{p-2+\left(\frac{-1}{p}\right)}{4};$$

$$nn_l = \frac{p - 4 - \left(\frac{-1}{p}\right)}{4};$$

$$rr_l = \frac{p - 2 + \left(\frac{-1}{p}\right)}{4};$$

$$nr_l = \frac{p - \left(\frac{-1}{p}\right)}{4};$$

Тепер доведемо теорему за допомогою описаних термінів.

Випадок 1:$(p \equiv 1(mod 4))$.

В цьому випадку $-1 \in Q_p$, тому вираз $A^2 - 4G \notin Q_p$ еквівалентний виразу $G + (-(2^{-1}A)^2) \notin Q_p$.

Також зазначимо, що $-(2^{-1}A)^2 \in Q_p$. Тоді, згідно [9], наслідок 2, кількість таких пар $(G, G + l)$, де $l \in Q_p$, причому $-(2^{-1}A)^2 \notin Q_p$, $G \in Q_p, G + l \notin Q_p$, дорівнює $rn_l = \frac{p - \frac{-1}{p}}{4} = \frac{p-1}{4}$.

Випадок 2:$(p \equiv 3(mod 4))$.

В цьому випадку $-1 \in Q_p$, тому вираз $A^2 - 4G \notin Q_p$ еквівалентний виразу $4G - A^2 Q_p \Leftrightarrow G + (-(2^{-1}A)^2) \in Q_p$, при чому $-(2^{-1}A)^2 \notin Q_p$.

Тоді, згідно з наслідком 2, кількість таких пар дорівнює rr_l, де $l - (2^{-1}A)^2 \notin Q_p$, тобто $rr_l = \frac{p-2+\frac{-1}{p}}{4} = \frac{p-3}{4}$. □

Висновки до розділу 3

В цьому розділі було отримано необхідні і достатні умови існування кривої у формі Едвардса, що є ізоморфною до заданої кривої у формі Монтгомері. Сформульовано теорему, на основі отриманих умов та наведено її строге доведення. Сформульовано теорему, що показує кількість еліптичних кривих у формі Монтгомері, які є ізоморфними повним еліптичним кривим в формі Едвардса та наведено її строге доведення. Розроблено алгоритм, що виконує ізоморфне перетворення (при виконанні умов ізоморфізму) кривої у формі Монтгомері у криву в

формі Едвардса та доведено його коректність роботи. Розроблений алгоритм було програмно реалізовано за допомогою ресурсів мови програмування $C\#$ на платформі .Net Framework 4.7.2.

ВИСНОВКИ

У ході даної роботи було проведено аналіз опублікованих джерел за тематикою еліптичних кривих в формі Едвардса, еліптичних кривих в формі Монтгомері, еліптичних кривих в формі Вейєрштрасса. Наведено опис модифікацій еліптичних кривих в формі Едвардса та їх властивості.

Аналіз особливостей еліптичних кривих в формі Едвардса показав за рахунок яких властивостей кривих підвищується швидкодія криптосистем.

Аналіз перетвореня еліптичних кривих в формі Вейєрштрасса в еліптичні криві в форму Едвардса та перетворення еліптичних кривих в формі Вейєрштрасса в форму монтгомері допоміг формалізувати необхідні та достатні умови ізоморфізму між кривими у формі Монтгомері та кривими у формі Едвардса, на основі яких будувались теореми.

Основними результатами можна вважати:

1) Необхідні і достатні умови існування кривої у формі Едвардса, що є ізоморфною до заданої кривої у формі Монтгомері та сформульовану теорему з доведенням, на основі цих умов.

2) Формулювання теореми, що показує кількість еліптичних кривих у формі Монтгомері, які є ізоморфними повним еліптичним кривим в формі Едвардса та її строге доведення.

3) Алгоритм, що виконує ізоморфне перетворення (при виконанні умов ізоморфізму) еліптичної кривої у формі Монтгомері у еліптичну криву в формі Едвардса з доведенням його коректність роботи.

4) програмну реалізацію алгоритму ізоморфного перетворення еліптичну кривої у формі Монтгомері у еліптичну криву в формі Едвардса, виконану за допомогою ресурсів мовипрограмування C# на платформі .Net Framework 4.7.2.

Метою подальшого дослідження є побудова критеріїв ізоморфізму еліптичних кривих у формі Монтгомері деякій скрученій еліптичній

кривій в формі Едвардса, та побудова аналогічних критеріїв ізоморфізму для квадратичних еліптичних кривих Едвардса.

ПЕРЕЛІК ПОСИЛАНЬ

1. Bernstein D.J. Faster addition and doubling on el liptic curves. — 3 edition. — 2007. — P. 29–50.

2. Edwards H.M. A normal form for elliptic curves. / H.M. Edwards // Bulletin of the AMS 44(3) – 2007 – С. 393–422.

3. Ковальчук Л.В, Бессалов А.В, Беспалов О.Ю. Алгоритмы генерации базовой точки с использованием критериев делимости точки кривой. — Прикладна радіоелектроніка, 2013. — С. 285–291.

4. Bernstain Daniel J., Birkner Peter, Joye Marc. Twisted Edwards Curves. //IST programme ynder Contract IST-2002-507932, С. 1-17.

5. Ковальчук Л.В. Рекурентні алгоритми обчислення кореню довільного степеню у кільці лишків. —Правове забезпечення системи захисту інформаціїв Україні, 1(25) вип., 2013. — С. 58–66.

6. Bernstein Daniel J., Birkner Peter , Joye Marc , Lange Tanja, Peters Christiane. Twisted Edwards Curves. IST Programme under Contract IST–2002–507932 ECRYPT,and in part by the National Science Foundation under grant ITR–0716498, 2008, PP. 1-17.

7. Morain F. Edwards curves and CM curves. ArXiv 0904/2243v1 [Math.NT] Apr.15, 2009, 15p.

8. Huseyin Hisil Twisted Edwards Curves Revisited / Hisil Huseyin, Koon-Ho Wong Kenneth, Carter Gary, Dawson Ed. // ASIACRYPT. – 5350. – New York: Springer, 2008. – С. 326-343.

9. Беспалов О. Узагальнення леми Гаусса про характери пар елементів простого скінченного поля. // Зб.наук.праць Інституту Кібернетики ім. В.М. Глушкова НАН України та Кам'янець-Подольського національного університету ім. І. Огієнка, випуск 15, 2017р., стор. 26-31.

10. Koblitz N. A Course of Number Theory and Cryptography.- Berlin: Springer, 1994. p. 139-200

ДОДАТОК А

Файл MainWindow.xaml:

```
<Window x:Class="TransformationAlgo.MainWindow"
    xmlns="http://schemas.microsoft.com/winfx/2006/
    xaml/presentation"
    xmlns:x="http://schemas.microsoft.com/winfx/
    2006/xaml"
    xmlns:d="http://schemas.microsoft.com/expres
    sion/blend/2008"
    xmlns:mc="http://schemas.openxmlformats.org
    /markup-compatibility/2006"
    xmlns:local="clr-namespace:TransformationAlgo"
    mc:Ignorable="d"
    Title="MainWindow" Height="450" Width="800">
<Grid>
    <Grid.RowDefinitions>
        <RowDefinition Height="206*"/>
        <RowDefinition/>
        <RowDefinition Height="213*"/>
    </Grid.RowDefinitions>
    <Grid.ColumnDefinitions>
        <ColumnDefinition Width="94*"/>
        <ColumnDefinition Width="3*"/>
        <ColumnDefinition Width="695*"/>
    </Grid.ColumnDefinitions>
    <Button Content="Generate Curve" Margin="0,44,40,0"
    VerticalAlignment="Top" Grid.Column="2" Grid.Row="2"
    HorizontalAlignment="Right" Width="109" Height="19"
    Click="Button_Click"/>
    <TextBox x:Name="inputA" Height="22"
```

```
Margin="281,56,295,0" TextWrapping="Wrap"
Text="Input A" VerticalAlignment="Top"
Grid.Column="2"/>

<TextBox x:Name="inputG" Height="24"
Margin="281,117,295,0" TextWrapping="Wrap"
Text="Input G" VerticalAlignment="Top"
Grid.Column="2"/>
<TextBlock HorizontalAlignment="Left"
Margin="70,56,0,0" TextWrapping="Wrap"
Text="Parameter A" VerticalAlignment="Top"
Grid.ColumnSpan="3" Height="16" Width="65"/>

<TextBlock HorizontalAlignment="Left"
Margin="70,117,0,0" TextWrapping="Wrap"
Text="Parameter G" VerticalAlignment="Top"
Grid.ColumnSpan="3" Height="17" Width="91"/>
<TextBlock Margin="70,201,6,0" TextWrapping="Wrap"
Text="Parameter d" VerticalAlignment="Top"
Grid.RowSpan="3" Height="16"/>
<TextBox x:Name="outputD" HorizontalAlignment="Left"
Height="24" Margin="281,193,0,0" TextWrapping="Wrap"
Text="Outgoing d" VerticalAlignment="Top"
Width="120" Grid.Column="2" Grid.RowSpan="3"/>

<TextBlock HorizontalAlignment="Left"
Margin="70,163,0,0" TextWrapping="Wrap"
Text="Mod P" VerticalAlignment="Top"
Grid.ColumnSpan="3"/>
<TextBox x:Name="Modular" Grid.Column="2"
HorizontalAlignment="Right" Height="24"
```

```
        Margin="0,162,295,0" TextWrapping="Wrap"
        Text="Modular" VerticalAlignment="Top"
        Width="120"/>

    </Grid>
</Window>
```

Файл MainWindow.xaml.cs:

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.Windows;
using System.Windows.Controls;
using System.Windows.Data;
using System.Windows.Documents;
using System.Windows.Input;
using System.Windows.Media;
using System.Windows.Media.Imaging;
using System.Windows.Navigation;
using System.Windows.Shapes;
using System.Numerics;
using System.Globalization;

namespace TransformationAlgo
{
    public partial class MainWindow : Window
    {
        public MainWindow()
        {
```

```
    InitializeComponent();
}

private void Button_Click(object sender,
RoutedEventArgs e)
{
    BigInteger ParA = BigInteger.Parse(inputA.Text,
    NumberStyles.AllowHexSpecifier);
    BigInteger ParG = BigInteger.Parse(inputG.Text,
    NumberStyles.AllowHexSpecifier);
    BigInteger ModP = BigInteger.Parse(Modular.Text,
    NumberStyles.AllowHexSpecifier);
    if (!CheckParameters(ParA,ParG,ModP))
    {
        outputD.Text = "Invalid parameters!";
        return;
    }
    BigInteger u1 = AlgoModel.SqrtMod(ParG, ModP);
    BigInteger c = BigInteger.Divide(ParA,
    BigInteger.Parse("3"));
    BigInteger outputDvalue = 3 * c - 2 * u1;
    outputDvalue = outputDvalue *
    AlgoModel.modInverse(3 * c + 2 * u1, ModP);

    while (outputDvalue > ModP)
    {
        outputDvalue =
        BigInteger.Subtract(outputDvalue, ModP);
    }
    outputD.Text = outputDvalue.ToString();
}
```

```
        private bool CheckParameters(BigInteger A,
        BigInteger G, BigInteger p)
        {
            bool Constraint1 = AlgoModel.LegendreSymbol
            (-BigInteger.ModPow(A,
            BigInteger.Parse("2"), p)-4*G, p) ==
            BigInteger.MinusOne;
            bool Constraint2 = AlgoModel.LegendreSymbol(G,
            p) == BigInteger.One;
            return Constraint1 && Constraint2;
        }
    }
}
```

Файл AlgoModel.cs:

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.Numerics;
using System.Collections;
using System.Text.RegularExpressions;

namespace TransformationAlgo
{
    public class AlgoModel
    {
        public static BigInteger RandomIntegerBelow
        (BigInteger N)
        {
```

```
    byte[] bytes = N.ToByteArray();
    BigInteger R;
    Random random = new Random();
    do
    {
        random.NextBytes(bytes);
        bytes[bytes.Length - 1] &= (byte)0x7F;
        //force sign bit to positive
        R = new BigInteger(bytes);
    } while (R >= N);

    return R;
}
public static BigInteger PositiveModular
(BigInteger value, BigInteger mod)
{
    value = BigInteger.Remainder(value, mod);
    if (value.Sign == -1)
    {
        while (value.Sign == -1)
        {
            value += mod;
        }
    }
    return value;
}
public static BigInteger SqrtMod
(BigInteger value, BigInteger mod)
{
    value = PositiveModular(value, mod);
    BigInteger k = (mod - 3) / 4;
```

```
    BigInteger res = BigInteger.ModPow
    (value, k + 1, mod);
    return res;
}
public static BigInteger modInverse
(BigInteger value, BigInteger mod)
{
    value = PositiveModular(value, mod);
    BigInteger i = mod, v = BigInteger.Zero,
    d = BigInteger.One;
    while (value > BigInteger.Zero)
    {
        BigInteger t = i / value, x = value;
        value = BigInteger.Remainder(i, x);
        i = x;
        x = d;
        d = v - t * x;
        v = x;
    }
    v = PositiveModular(v, mod);
    return v;
}
public static BigInteger LegendreSymbol
(BigInteger FirstOperand, BigInteger SecondOperand)
{
    FirstOperand = PositiveModular
    (FirstOperand, SecondOperand);
    if (FirstOperand == BigInteger.Zero)
    {
        return 0;
    }
```

```
    if (FirstOperand == BigInteger.One)
    {
        return BigInteger.One;
    }
    if (BigInteger.Remainder(FirstOperand, 2)
    == BigInteger.Zero)
    {
        return LegendreSymbol(FirstOperand / 2,
        SecondOperand) * BigInteger.ModPow
        (BigInteger.MinusOne,
        (SecondOperand * SecondOperand - 1) / 8
        , FieldMod);
    }
    if (BigInteger.Remainder(FirstOperand, 2) !=
    BigInteger.Zero && FirstOperand !=
    BigInteger.One)
    {
        return LegendreSymbol(BigInteger.Remainder
        (SecondOperand, FirstOperand), FirstOperand)
        * BigInteger.ModPow(BigInteger.MinusOne,
        (FirstOperand - 1) * (SecondOperand - 1) /
        4, FieldMod);
    }
    return BigInteger.Zero;
}

public static string ConvertToBit
(BigInteger decimalNumber)
{
    BigInteger remainder;
    string result = string.Empty;
```

```
            while (decimalNumber > 0)
            {
                remainder = decimalNumber % 2;
                decimalNumber /= 2;
                result = remainder.ToString() + result;
            }
            return result;
        }
    }
}
```

Файл EdwardsModel.cs:

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Numerics;
using System.Text;
using System.Threading.Tasks;

namespace TransformationAlgo
{
    class EdvardsModel
    {
        public BigInteger ParD = BigInteger.Zero;

        public EdvardsModel(BigInteger parD)
        {
             this.ParD = parD;
        }
        class Point
        {
```

```
    public BigInteger x = BigInteger.Zero;
    public BigInteger y = BigInteger.Zero;

    public Point()
    {
    }
    public Point(BigInteger X, BigInteger Y)
    {
        this.y = Y;
        this.x = X;
    }
    public override string ToString()
    {
        return $"({x}, {y})";
    }
}
static Point getRandomPoint
(BigInteger Modulus, BigInteger parD)
{
    BigInteger x, y;
    while (true)
    {
        x = RandomIntegerBelow(Modulus);
        y = (1 - x * x) * AlgoModel.modInverse
        (1 - parD * x * x, Modulus);
        if (AlgoModel.LegendreSymbol(y, Modulus) == 1)
        {
            y = AlgoModel.SqrtMod(y, Modulus);
            Point point = new Point(x, y);
            return point;
        }
```

```
            }
        }
        static BigInteger RandomIntegerBelow(BigInteger N)
        {
            byte[] bytes = N.ToByteArray();
            BigInteger R;
            Random random = new Random();
            do
            {
                random.NextBytes(bytes);
                bytes[bytes.Length - 1] &= (byte)0x7F;
                R = new BigInteger(bytes);
            } while (R >= N);

            return R;
        }
    }
}
```